Privacy & Security Workgroup
Draft Transcript
February 18, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning and welcome, everybody, to the HIT Standards Committee Privacy & Security Workgroup. This call is open to the public, and the public will have an opportunity at the close of the meeting to make comments. Just a reminder to workgroup members to please identify yourselves when speaking. Let me just do a roll call now. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Findlay?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro? Dave McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Gina Perez? Wes Rishel? Farzad Mostishari? Walter Suarez?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. This Walter Suarez.

Judy Sparrow – Office of the National Coordinator – Executive Director
Aneesh Chopra? Chris Brancato?

Chris Brancato – Deloitte – Manager, Health Information Technology
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Moehrke?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Ed Larsen?

Ed Larsen – HITSP

Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Sue McAndrew? Kevin Stein? John Halamka?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I got a message from John Halamka that he couldn't join us today, but he did send me a couple of comments.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Thanks. And on the line from ONC is myself, Deborah Lasky, Sarah Wattenberg, and Kathy Kenyon. With that, I'll turn it over to Dixie and Steve.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you all for dialing in this morning, and thank you also for your contributions and taking the time to review the IFR and to send me comments. We got quite a few comments, and have attempted to fold them all into the document that I sent out yesterday. Today, I'd like to just go through this document, and particularly paying attention to the recommendations. Some of the comments I really had to make up the recommendation, and so it's my recommendation, and I'd like to hear your thoughts on it.

Are there some overall general thoughts that you'd like to express at the beginning? Okay. I can tell you that the only comment I got, John Halamka, is that fact that we have included this last section where I included the comments about administrative transactions, and that incorporates comments from Walter and Anne. And the other one is newborn screening, which is Sharon Terri's comment.

John's comment was that neither of these are related to the IFR itself, not only that they aren't privacy and security, but that they really should be forwarded to the HIT Policy Committee. And specifically the administrative transaction, he suggests, be forwarded to the policy committee's subcommittee on meaningful use or the meaningful use workgroup. And he also felt that it illustrated a misunderstanding of meaningful use and certification.

I'm just reading his e-mail. "In Boston, it is a combination of our home built EHR plus NHIN that will be certified for administrative transaction exchange. A combination of modules to accomplish the tasks is just fine."

Let me start off on that. What would you guys like to see happen to these two comments?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
This is Steve. I must admit. I didn't quite understand why they were there either, but that's just mostly ignorance that I didn't quite understand the issue, so I'll just weigh in that if someone can explain that part, maybe others would benefit from that on the call as well. I don't know, Dixie, if you want to try your hand at that, just a brief explanation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure, sure. The administrative transactions is a meaningful – well, the administrative transactions is a meaningful use measure that you have to do 80% of your administrative transactions electronically. And the administrative transactions are those transactions that are defined in HIPAA, you know, like claims and eligibility, etc. There are about seven, I think, transactions.

And what they're saying is that they don't believe that that – really what they're saying is that they don't believe that measure should be in meaningful use and for a number of reasons. Walter, do you want to go through this? You really are the one who articulated explicitly the three reasons, the clearinghouse, etc. Walter, are you on mute?

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter, are you there?

W
His line disconnected. He's dialing back in.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Dixie, was there anyone else who commented on that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, both he and Anne Castro. Anne is not on the line. He pointed out correctly that the HIPAA allows to do these transactions through a clearinghouse. The HIPAA explicitly says that you don't have to implement electronic transactions, these EDI transactions yourself. You can send your claims to a clearinghouse and have them do it. He's right. It does explicitly say that.

The second was that both of them – it's something that both he and Anne pointed out that EHR systems today don't typically do administrative transactions. Those are claims and eligibility and coordination of benefits. All of that are usually done by backend administrative systems, not by EHR systems. Then the third is that if – now this one, if you don't understand ARRA, it probably would be a little bit difficult.

ARRA says that – has a new provision for accounting for disclosures, and if you send information between enterprises from an EHR system, and it has that in it, that constraint. If you send it from an EHR system, then you have to do an accounting for disclosures. What he's saying here is that if in fact you do any of these HIPAA transactions—claims, eligibility, etc.—from an EHR system, then it immediately comes under the, you know, it will be required to be considered a disclosure.

Now my personal opinion is that that's part of what that requirement was anticipating, but those are the three arguments. And they recommend that the administrative transaction meaningful use measure be removed as a measure, and that the criteria be removed relating to it, that criterion standards be removed as well.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, this is David. I think these points may be valid points, but I don't know that they belong in our response on privacy and security issues. It really is a meaningful use question.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
How about if I take those two, just that last section, and create a second memo like this that's just to John Perlin, John Halamka, and say that these were questions that our workgroup members submitted, or comments that they submitted, and we request that they be forwarded to the policy committee?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's okay with me. I mean, I think they're good points. I just don't think they should be mixed in with the more specific security questions that we were asked to address.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. I agree. That's why I put it at the end because it really, any other place, it really interrupted the whole messages and what we're trying to do. But on the other hand, there are members in our workgroup, and I want their concerns to be known, you know.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, this is Walter. I'm trying, with separating this. As I started at the beginning of my comment, this is not a topic for privacy and security, but it's a topic for the IFR indeed, not just meaningful use, because the IFR establish a standard or two standards: one for claims and one for eligibility or for the HIPAA transactions. And so establishing the standards on the IFR, that gives an impression or at least a perceiving sense of being needed for meaningful use creates that confusion. That's why the recommendation is not just on the NPRM side to eliminate this from having it as a meaningful use measure, but also from the IFR from setting it up as a standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I see your point. Let me modify … if we extracted and put it in a different memo and asked them to forward it to the appropriate parties, and leave it up to them.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I think that won't be a problem.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I'm going to do. I highlighted just for you guys, and I'll remove it to send our final, but I did, as Walter took all of our comments and put them in a spreadsheet for me, which made it a lot easier for me to see what everybody was saying about each certification criterion and each standard. And, as I wrote the comments about what was questions two and three, there was a lot of duplication, and so I just combined them in here as one. Whereas we had seven, we now have six, and that's why.

The only general comment has to do with, it's something that we've actually spent considerable time discussing, which is the fact that, in the preamble of the IFR, it contains a table, Table 2B, which contains the functional standards, all the standards expressed in functional wording. Then for a number the standards, not all, it has an e.g., and it mentions particular technical standards that are managed by standards development organizations like the transport layer security and like IT Set, and SAML, etc. In the body of the regulation, those e.g.s don't appear. The standards are simply functional statements with the exception of the hashing function is the only one that's mentioned in the body itself.

We've talked about what we should do with these. You may recall, we asked Judy to find out whether they could be put in an appendix, etc. In David McCallie's comments, he mentioned that that really should be the responsibility of certifiers, and that gave me the idea of a recommendation that as the ONC developed the certification program, they include a framework and processes for specifying and maintaining this list of example technology standards that meet the function standards specified for EHR certification. I'm interested in hearing your thoughts about that approach. David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. This is David. I like it. I like the way you worded it. I circulated it internally to John Travis, who works on our certification efforts, and he thought it made a lot of sense as well and was consistent with what he'd seen sort of evolving in that space, so I like it.

I did raise the question in e-mails with you about some notion of establishing a base level of functionality that the certification choices wouldn't drop below, and I don't think that's easy to do with something like encryption because it's hard to define functionally what a base is. But I also don't think it's a problem. I

think that the market's understanding of how encryption technologies evolve is pretty straightforward, and they get better over time, and people understand what that means, so I don't know that we need to be more precise or try to invent some kind of arbitrary base. But that would be for NIST maybe to decide.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
See, I kind of thought, the reason I didn't put that, I think that that's what the functional standards do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, just how would you functionally specify that? There may well be one, and I'm just naïve to knowing how to do it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Like the encryption standard, that's exactly what it is, you know, because it specifies pretty much, as John Moehrke has pointed out, the way it's stated, it can only be met by AES, so that's kind of, I think, what it's attempting to do. I agree that not all of them do that though.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But do you think that we should specifically require AES or say that it has to be at least as good as that, and to be determined by the certification process, as that evolves over time?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Either of those things would be better than what's there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Agreed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I don't like what's there either, quite frankly, but it's hard. Well, that's a different topic. Maybe we should add in this one that the functional standards should be stated such that the functional standards should establish the base level functionality.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
In general, with all of these standards, almost all of them, not just limited to security, the technologies and approaches will evolve, and the regulations have to be written ideally in such a fashion that they allow vendors to do a better job in the future without having to be constrained to a point in time when somebody wrote a regulation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree with you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's just a generic problem, and I don't know the best way to deal with that, but certainly encryption will get better, and we should be free to use better approaches, as they evolve.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. And I think we're especially constrained because we can't recommend NIST guidelines and standards. NIST is kind of the – for the country, both federal and private industry look to NIST standards for encryption and kind of follow those. But I think, in an ideal world, that's what you would specify as your standard is whatever NIST recommends from the federal government should be. But we can't do that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Dixie, this is John Moehrke. Why do you think that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Because I've been told explicitly that, yes, time and time again. We've tried, when we were doing standards, when we were developing the standards, we tried to use several NIST and were told we couldn't do that.

Let's go to the specific questions. Number one has to do with the general approach of this is where we express our concerns about the certification modules. There are a couple of problems, you know, if you specify. What the document says is an EHR module is something that meets at least one of the certification criteria. As we all know, we have security certification criteria. So the question arises is, if I submit something that only meets one certification criteria, and really has no health functionality, can it be evaluated in an EHR module?

Then the converse of that is, if I have an EHR module, and it does no security functions at all, can that be certified? Then the third problem, if you have EHR modules, each of which either provide their own security or assume that somebody else will, you can't possibly have sound enterprise wide security.

Building on a comment really that Ed Larsen sent, what I recommended was that, well, first, the A recommendation down there, which should be one, but it says A, is a comment that David McCallie made about the wording of it. It wasn't clear. As you read through the whole document, it's clear that they're proposing to certify complete EHRs and EHR modules. Then what an eligible provider or professional or hospital needs to present to CMS to get reimbursed is their solution, which is certified EHR technology. It says that if that organization uses multiple modules to form that certified EHR technology, it's up to them to kind of make sure everything works together.

David commented that the wording didn't really convey that precisely, and so we've recommended a change in the wording to certified EHR technology means a complete EHR or a set of EHR modules either of which, either the set or the complete EHR. It's a very awkward sentence either way, but he was correct. It wasn't clear whether it meant the complete EHR or each module or whatever. Have you looked at that wording and whether this fixes the problem, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I certainly think it's a good step in that direction, and I agree that it's going to be awkward because there isn't a clear definition anywhere yet as to what these modules are, and whether or not there will be kind of rigid categories of modules, in which case one could, on a module-by-module basis, or category-by-category basis, specify specific security requirements, or whether it's going to be up to the market to figure out what the modules are and the security issues essentially are forced to become addressable issues where judgment is required based on what actually emerges. I don't' think we know the answer to that. So, in the meantime, we're stuck with this ambiguity. I think the spirit is clear is that the system as a whole has to be secure, but how to put that in regulatory language is over my head.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think it's clear that they don't intend to certify the entire set of modules. They explicitly say that's up to the provider organization. But what I've recommended is just what Ed Larsen suggested, but I've expressed it using the same approach that the HIPAA uses. And what I've recommended is that if an EHR module is submitted for certification that all of the privacy and security criteria become addressable for it. So if the vendor or the hospital or whomever is submitting this module for certification, would need

to go down that list of certification criteria and explain how that would be, that requirement would be met with their module, yes, with their modules.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that makes sense. I think there's a good basis for that approach. It's worked in the past with similar issues and HIPAA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
With HIPAA, and it's consistent with HIPAA.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that that's the best we're going to do. Okay. Let's go to number two. This has to do with the reasonableness of the certification criteria, and we got more. Well, we got a lot of comments about this and the standards. But I think, because this was earlier in the list of questions, this was question two and three.

The first one, it was the audit log, the fact that it has alerts in there, and HIPAA – neither HIPAA nor ARRA calls for alerting, and basically to do alerting, you have to do real time processing of audit logs, and have the greater decision support. And so I recommended that we remove this certainly for stage one.

And the other point that somebody made was display and print, and we recommended that the audit records be displayable and printable in a structured format for human review. The comment there was that some – let's see – oh, that it was not specific, not sufficiently specific. The original requirement is an electronic display and print all of the specified set of recorded information upon request or at a set period of time. The comment was, that's not specific enough for testing, and so the recommendation is to require that audit records be displayable and printable in a structured format designed for human review. Comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I like that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes. This is Steve. That's terrific.

Dixie T.
All right. The integrity, this one is one that it wasn't clear. You know, when you send information over the Internet, there is a complete … packets that go over the Internet, and there are methods that are commonly used … verify that the…. But verifying the integrity of the document that you're actually sending and, as we've expressed here, the payload of a message is beyond what's commonly done, and it does require considerably more processing and more functionality than most systems have. This is a comment from David. And so he requested, and this is what our recommendation is to clarify that detect all duration in transit requires only that the integrity checks be performed on the transmission channel, and that the integrity of the payload can now be independently verified.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I'm still comfortable with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The next one is on authentication. This one is where we had the most issue, I think, of all the criteria and standards, quite honestly. We recommended that integrating the healthcare enterprise, cross enterprise user assertion profile, and the security assertion markup language that it uses be standards for 2013. What that profile and those standards do, those are used or SAML in particular is used to implement single sign on. And, most commonly, single sign on across an enterprise. Virtually, it could be literally, I don't know of anybody who uses SAML to do single sign on across companies, multiple companies, multiple enterprises.

M
By the way, Dixie, I do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You do? We also know that there are no real models for sharing information. There's no vocabulary for sharing information. Maybe it is something that we can target for 2013, but basically we disagree with their including it for 2011.

M
I absolutely agree with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. And the other problem that we had is that the transport layer security does three things.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, this is Walter. On that point, on the previous point, I think their recommendation should roadmap this to 2013. The actual recommendation doesn't – it just says remove the requirements, but it doesn't … a roadmap to move it to 2013, which I think would be appropriate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. I'm going to say, and reconsider for 2013. We'll see how the industry does.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I may be confusing different parts of the actual regulation, but in 170.210 subpart D, cross enterprise authentication, the reg says across enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails must be used. That seems reasonable to me.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I said in my comment, but when you go to the XUA profile, and even at the introduction to the XUA profile, it makes it quite clear that it's between enterprises.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But there's nowhere in the actual reg that mentions XUA, is there?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Yes, there is in Table 2B.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But that's in the commentary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is back to the confusion about the fact that they talked about e.g. standards doesn't actually have regulatory power, does it?

John Moehrke – Interoperability & Security, GE – Principal Engineer
David, I agree with your observation, but I think it's still better for us to make sure we're clear we help them clarify what we really would prefer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
John, I agree. I just wanted to make sure I wasn't missing something somewhere.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Because the spirit of the regulation actually seems pretty consistent with what we're asking for.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. In fact, if you read my original comments, that's what I said. If you really just read the functional statement itself, it sounds like something like Kerberos, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right. It just says you've got to know who you're talking to when you go across enterprises, which is a pretty reasonable statement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. Right, but the fact that in the preamble they link it to XUA.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's where we have heartburn, all of us, I agree. And so I think our comments should stand, but if they ignored it completely, I actually think we're on fairly good ground.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, actually, I think there is some concern, even with the minimal text in the regulation because it does not recognize that, in many cases today, organization-to-organization authentication is sufficient and that there is, in many cases today, no need to pass user identity at all.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I see. That's an interesting point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That is a good point, John. That's true. That is true. So the other part of what we recommended, what I started to say about TLS, transport layer security, which they definitely have in their standards, it's

basically to set up a trusted channel between two enterprises, between an enterprise and a person or, you know, for various reasons when you buy things on the Internet.

The first thing it does is to authenticate at least one of the two endpoints, and whether it authenticates both or one is a policy decision, but the TLS itself has the capability to authenticate both endpoints and set up an encryption for a across the channel and integrity protection across the channel. Several of us suggested that the standards needed, the standards know the criteria address that number one part of it, which is critical to TLS, which is the authentication of the endpoints. Several of us recommended that they replace this XUA SAML with the authentication, the requirement to have the capability to authenticate endpoints of exchanges between enterprises using TLS, well, TSL or IPSec is what it is. But basically to replace this single sign on requirement with the requirement that you make sure you know who you're talking to, to begin with, before you set up an encryption….

John Moehrke – Interoperability & Security, GE – Principal Engineer
Dixie, that I thought did a very nice cleanup of the point I just made where, in many cases, organizational authentications should be sufficient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I certainly agree with the language, Dixie, and clarification. But again, just reading literally what it says in Point D, whatever that 172.10D, it says a secure transaction that contains sufficient identity information such that the receiver can make access control decisions. That doesn't imply necessarily that it's person level identity. It could be group. It could be entity. And just saying sufficient identity information, it's almost a meaningless statement, really. But nonetheless, I think our clarifications and removal of the XUA in the commentary is worth sticking with.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I agree with you on both counts, actually.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I've seen universal reaction to that statement that it should not be there, so I don't have any problems that we're getting out of line at all.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. The next topic is encryption. They have, it's rather confusing here. They have three sections. They have the U is encryption as a topic. Then they have one, which is general encryption, and two, which is exchange encryption. The one is just kind of a general statement about encryption. Let me bring this thing up so that I can see it, like David is.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I've got so many papers spread out in front of me, it looks like I was in a windstorm or something.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. I think I've got this thing memorized. I thought I had it memorized, but maybe I don't. I think the first one says, let's see, here we go. Okay. The first general statement, the certification criterion for general encryption is encrypt and decrypt electronic health information according to user defined preferences in accordance with the standard specified in, and that standard is basically AES, and the exchange is to encrypt and decrypt electronic health information.

I have two problems with this. Number one is that it's not clear, and we hear people talk about this a lot, whether this applies to the capability, not actually doing, but whether products need to have the capability

to encrypt data at rest. And the HIPAA requirements security rule itself clearly specified two separate encryption requirements: one for data at rest, and one for transmission.

I felt it should make it clear that products need to have the capability. That doesn't mean that they always have to encrypt. But they have to have the capability to encrypt data at rest, and that they should make that clear.

Then the second thing was this user-defined preferences. I thought it's not consistent with how encryption generally is done because usually whether to encrypt or not is an enterprise wide policy thing, not each doctor deciding whether they're going to encrypt something or not. So I recommended revising the general criterion to read what I have there. "Encrypt and decrypt electronic health information according to entity specified policy and risk mitigation strategies for protecting data at rest and in motion, in accordance with the standards."

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, I like the wording. I think that's essentially saying it's addressable, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I'm kind of concerned about this leaking. This is leaking into areas for which it really needs to be addressable.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That was going to be my question is do we want to be consistent and use that language, addressable. I don't know the technical, legal definition of addressable, but what you wrote sounds to me like what I hear in my head.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't know what you mean. Of course it would be addressable for an EHR module, right. But let's say a complete EHR, as they defined it, is submitted for certification. No, I would not consider this addressable. I would consider it a requirement.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But the requirement is that it be used according to an entity's decision about risk assessment.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. It says nothing about whether it's used or not. Remember, that's meaningful use. This is if you submit a product for certification, it would say that that product must be capable of encrypting information if the enterprise, for example, wants – let's say they decide … and that's why I put the policy and risk mitigation strategy. Let's say they handle – one of their departments does psychotherapy notes, and they decide they want the directories, folders, whatever you want to call them that have psychotherapy notes encrypted. Then the product should be capable of doing that. And that doesn't mean that it can't use an external module to do that. It just says that the product that's submitted for certification needs to be able to do that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's where I was really headed with my question. Does that, in your mind, mean that all the products have to be capable of every possible combination of how someone might request that encryption be done?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, that's my concern as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, you can't possibly do that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That's very burdensome.

M
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you couldn't, and also, I was thinking through like whole disk encryption. That's totally different. You'd get a totally different product to do that. This would just be that the capability to support encryption.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But when you say it's that open-endedness of the capability. I mean, if that meant somewhere, somehow, you have to be able to encrypt data at rest, that's one thing. If it means the purchaser of the module can tell you how to do it, and you have to respond, that's something completely different.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Obviously it can't be B. How could we change it so it's not B?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. It's that word capability that is ambiguous. John, do you have any suggestions?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I'm really concerned about the requirements for data at rest because the actual implementation of addressing risks for data at rest is a very involved risk assessment and mitigation plan, and you certainly see things like NIST 800-111 that are huge explaining this. I mean, if it was just as simple as, encrypt everything everywhere, there wouldn't need to be such large documents. I would really prefer we stay away from data at rest. It's already dealt with in HIPAA. It's already dealt with within breach notification, and I think the market forces are already driving the appropriate behavior. By putting in a mandate for encryption of data at rest, we circumvent a risk assessment.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
This is Walter. I don't think it's really mandating encryption for the data at rest. It's mandating a specific approach to encrypting if the decision is to do encryption when data is at rest. It's an issue, too, in my mind because, yes, I don't think data at rest necessarily should be covered. I agree. We don't necessarily have to or should include in these regulations the standard for data at rest. I think the requirement is already taken care of, as John, you said, in the HIPAA regulations.

I think concentrating on the data in motion, I think the challenge is if the statements are so open and broad that any type of encryption capability that meets the general criteria can be used, and that's not promoting interoperability because, first of all, systems will have to be capable of handling multiplicities of ways of doing this. Secondly, entities will have to, on a one-to-one basis, agree with each of their trading

partners on doing it one way or another or in different ways. And so, at the end, this is not promoting interoperability.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You're getting into the standard, but the point here is going back to John's comment. Yes, it's a requirement of HIPAA. Therefore, I mean, that's what we've been trying to do is specify certification criteria that would help an enterprise comply with HIPAA. If HIPAA requires the capability to encrypt data at rest, I think we should have certification criterion that says the products have to help them do that. Secondly, the reason why I could, and maybe it doesn't do it, but my intent was, with the phrase "entity specific policy and risk mitigation strategy", that means that when they do their security risk assessments, which is required under HIPAA, that they decide what they want to encrypt and how they want to encrypt it.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Dixie, I think, as part of an NPRM statement, that would be perfectly fine. But because this is a certification criteria, as David has pointed out, the EHR has to presume all possible policy choices, which means all possible ways in which data is at rest.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I think we should be saying.

John Moehrke – Interoperability & Security, GE – Principal Engineer
But I don't think….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree, by the way, that that phrase is really an NPRM type phrase, not a….

John Moehrke – Interoperability & Security, GE – Principal Engineer
It does not help at all with the certification criteria to put that phrasing in.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But what I was trying to replace there, John, is this user defined preferences, which I think you would agree shouldn't be in there because encryption … be totally up to the user.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I'm okay. I absolutely agree that the word user is unclear. I think they actually did intend it to mean the healthcare provider organization.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The entity.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. But because it's unclear, I think, yes, absolutely, let's make it clear.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If we'd replace that with entity, would that do the trick?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, I would just like to stay away from data at rest simply because there are far too many ways in which data is at rest. If you focus purely on the transport, we can focus more on the transactions that cross

organizational boundaries, which are the high risk transports. There, I think we can be rather clear. But the data at rest is really troubling.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd be okay with this actually if we changed this one to encrypt and decrypt electronic health information according to entity defined preferences in accordance with the standards.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Would that be okay with you, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Would you say that again, Dixie, just one more time?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What we would change is user to entity. Encrypt and decrypt electronic health information according to entity defined preference in accordance with the standard.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That sounds okay. The essence is what we're saying is that the product has to be capable of meeting HIPAA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I mean, that's what it boils down to because obviously it has to do that, or it couldn't be deployed. Maybe the certification process need not be any more specific than that because there is, as John points out, volumes of stuff on what that means.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Let's just do that. I'm happy with that. That's fine. Then I'm going to delete this. This recommendation will say, "Revise the general criterion to read: Encrypt and decrypt electronic health information according to entity defined preferences in accordance with the standards." Okay. I'm happy with that. That's fine.

Accounting for disclosures, I really like John Moehrke's comment about this. I think it's really important, and I hope they pay attention to it. And we first wanted to acknowledge that they're clearly developing the NPRM right now, but the essence of his comment was that you don't really want to require that they capture the reason and the description and all the stuff in real time. But that in fact, you can get better accountability of disclosure through post processing in many instances, and what he basically was saying, make sure that it allows for. John, would you like to add anything more to that?

John Moehrke – Interoperability & Security, GE – Principal Engineer
You did good.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You did good too. Really good comments, so I've recommended that we revise it to read, "Create a record of treatment, payment, and healthcare operations, disclosures," the italics is theirs. "The date,

time, patient information, user identification, the description of the disclosure must be included in the accounting." The intent here is to make sure they don't lock in some concept of having to select this entire accounting in real time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Say that last sentence again, Dixie. It got garbled. You don't want to lock in what?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We don't want – we want to help them avoid creating a rule that would require the accounting of disclosures in real time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So if we say create a record, and that it must include, in the accounting, these elements, I think that'll do that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That part, I totally agree with. The enumeration of the items to be in that record, are we concerned that that might be either too broad or too narrow or too static?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's in the standard. This is just the certification criteria.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Okay. All right. I got it.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That is a standard that is in the HIPAA regulation for accounting of disclosures. I would just suggest adding one word including in the accounting of disclosures. I would add, included in the record of accounting of disclosures, so that….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So it's parallel with the first of the sentence, you mean.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Included in the record of accounting of disclosures. Agree, everybody?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. Let's look at timely access. This is here because our working group is really responsible for representing consumer issues as well, and so this is one of the consumer criteria. And Steve and I have gone back and forth on this one a bit, and I found the term "online access" problematic because many people would read that as meaning real time access to the real patient record that Kaiser is using, for example.

On the other hand, other people might read that as providing patients a view of something, online view of something, but not the capability to download it to their USB drive or something, right? And the HIPAA rule or the ARRA gives them a right to "an electronic copy". So I don't think online access captures the notion of electronic copy.

Also, the PHR, ARRA also says that they have a right to say, to request that their provider send the record to somebody else, like a PHR vendor. Quite honestly, I think the whole notion of sending it to a PHR needs to be addressed by the vocabulary messaging people as well. But the recommendation that Steve and I came up with was revise it to read, "Enable the consumer to provide patient/consumers with electronic access to a copy of their clinical information," so that it's clear that it's not an online access to the real, original record. A copy of their clinical information, including, at a minimum – minimum is in the reg already – and adding, "And to download their personal health information in a user-friendly and understandable format." And then the second is to establish as a priority for 2013 the specification of messaging and vocabulary standards for sending or transferring the electronic record to a PHR vendor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. Somebody else wanted to speak?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes, this is Steve. I was just going to add that I think it's critical, this underscored that term online access be very clearly defined, frankly, in both the NPRM and the IFR. There just needs to be a very consistent use of these words because we live in a changed world, and that term means different things to different people, and can be broadly defined and narrowly defined.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. You remember, even in our committee, we had a conversation one day about whether you had to provide online access to lab results, as they become available. I think we do need to clarify that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Let me preface my comment by saying there is no one who is a stronger advocate of consumer having access to the record than I am. In fact, I wouldn't give it to the states at all, so you guys know where I stand. So do not take this as I'm opposed to guaranteeing the consumer a right to a copy of their record. But I want to point out that online access and having a copy of your record could in fact be independent and both valuable activities. As long as I'm guaranteed that I can have a copy, that I can obtain a copy, then a quick view online is in fact, in many ways preferable to downloading a copy and having to put it somewhere before I can view it.

I'm thinking bank account. I can pull out my Smart Phone and get a quick view of my balance, and of recent transactions. If I want, I can download a copy to load into a local Quicken database, but in fact I never actually do the latter because I'd prefer the quick view that the bank provides for me. So I don't think we should exclude the notion that read only online access is valuable. We just have to insure that they can obtain a copy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. That's what I was trying to do. So if you have any recommendations, you know, what I was trying to do is exactly what you were saying that they could view it, but in addition, they could download a copy because that's what the law requires.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I would just simply say that we should stop at the word copy. As soon as you add the word "download", you start to muddy the waters.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I would use the word "obtain" instead of "download" or just say "obtain a copy".

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Obtain, okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Because you could get that. They could mail it to you securely. They could hand it to you on a thumb drive. There are a variety of ways that….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but obtain doesn't capture electronic.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, but….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Obtain an electronic copy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I guess I was interpreting electronic to mean that what you ended up with in your hand is computer readable. It doesn't necessarily have to come to you via an electronic channel. It could be handed to you on a disk drive.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, but to be electronic, what you end up with your in your hand has to be electronic.

W.
But you can say obtain electronically their health information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But you don't even have to obtain electronically. If they go to the doctor, and the doctor gives them a CD with an electronic copy of their record, that meets the law.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think you're right, and that's one of my concerns with the second item is that, in many cases, we have to recognize these portable CD-ROMS, USB sticks. Those are not being transferred or sent.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But then you can say to download their personal or to obtain their personal health information in an electronic form.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
In a user-friendly electronic or something.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I'm concerned about the user-friendly too because … that … user-friendly.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes….

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't to stop at user-friendly because, quite honestly, the XML forms that are being looked at are not at all user-friendly. But yet, if you want to convey the actual data between two providers by way of a USB memory stick that the patient carries, you don't want to convey it in a user-friendly format. You want to convey it in a doctor friendly format.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I agree. I think user-friendly, you know, of course becomes an interpretation issue for certification and for other purposes. So I would just say, and to obtain their personal health information an electronic form, period.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Correct.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Well, let me, I mean, the term user-friendly, I think, is just colloquially understood to mean that if you have the records in a form that is really very physician and provider oriented, and not at all "user-friendly" to the consumer, that that is not serving … the law.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I'm concerned about both ways and, indeed, I think it should be user-friendly, but it should also be full fidelity. The concern I have is if we just put in user-friendly, we start to cut off the legs of being able to use the data for any form of analysis, even at the PHR.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's why I added number two, but could we capture that, some notion of – well, that's not…. What you wanted is an electronic form in a format suitable for the intended recipient. But you can't test that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think the spirit of the original language was covering both those cases, so the online access was the user-friendly part, and the electronic copy was the machine readable part. I think maybe we've moved the wrong direction by getting rid of those two distinctions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

How about if we put up here, if we left online, but we changed? How about if we said provide patients/consumers with online access to a view of their clinical information, or electronic access to a view of their clinical--? I don't want it to look like, because if I were Kaiser, I sure wouldn't, or if I were VA, I wouldn't want this requirement to sound like I had to provide consumers an access to their record that the doctor's use on a day-to-day basis to make decisions. They want to provide consumers access to a view of records that they choose to make available.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I agree with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. That may be where we are today. I think, in the long run, we're going to end up with consumers have access to the record. I think that's inevitable.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, the long-term objective, not the short-term, is everything.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
And there's nothing behind….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm not saying not everything. What I'm saying is, for example, here's a good example. Labs always send a preliminary result first, and then they send a confirmed – or often – and then the send a confirmed result second. I don't think it's to the consumer's best interest to see the preliminary results. They want the final result. A doctor could have need for the preliminary result, and that is sent to the doctor, but the consumer should have access to their entire record. But the entire record, once it's confirmed, not as the doctor is entering the notes in real time, is halfway through. It's not the same record, but they should have access to the complete record once it's confirmed.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I agree. I think there's less and less concensus around that. In other words, there are a couple of states that require that physicians sign off on it first, and I think those are all going to go away in the long run, but I don't think it's our business to specify that kind of behavior in the security document, right? That's really meaningful use.

Sarah Wattenberg – ONCHIT – Public Health Advisor
Yes. This is Sarah Wattenberg too. Those, I think, are – David, I agree with you. I'm on the privacy and security workgroup, and a lot of those issues are sort of being discussed now at the policy level in terms of there are many states that actually allow patients to have direct access immediately. I think the more generic and basic, the better.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. I think the issues that we should wrestle with are, and maybe some of these are not quite in our purview, but are issues like what does machine readable mean? And what does … well, I don't know. I guess the language of online access and copy are in the statute, are they not?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, the copy is not. It's just online access. Oh, in the statute itself.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
In ARRA, yes. ARRA gives you a copy. I mean, HIPAA gives you a copy, an electronic copy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, HIPAA gives you a copy, but it doesn't have to be electronic.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But then ARRA goes further and says….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
ARRA adds electronic copy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. So we can't, I mean, that's there. Do we need to say anything more than that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I don't think we do, actually.

Sarah Wattenberg – ONCHIT – Public Health Advisor
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think what we need to say is enable a user to provide patients/consumers with electronic access to a copy of their clinical information, and I think we should add, "and to obtain an electronic copy of their personal health information," – oh, "obtain a copy of their personal health information in electronic form."

John Moehrke – Interoperability & Security, GE – Principal Engineer
I'm okay with losing the word download if it's problematic. But it was the focus of a lot of discussion at a couple of meetings, and the import behind those discussions is that really just thinking very simply for the benefit of the average consumer/patient, what we have to make sure is that there is a simple, online, download button that they can click on that either prints that page or prints some part of the full record. This is just a functionality, consumer friendly functionality that we want to signal, I think, in some way, but we don't have to bog down in it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But you don't want to require, and the law doesn't require that say a one doctor clinic provide a Web site where people can view their records. The law says that if I go to my doctor, who is a single physician practice, and I ask her to give me a copy of the record, she could give it to me on a CD.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. Right. I agree with that.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst

Yes. I think, as long as we make sure that can happen, because the words that you have today in the document, I think, would preclude that kind of a solution.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I think we have to remove that download. At a minimum, it's got to be something like obtain.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Obtain a copy of their personal health information in electronic form.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The other thing is, I think the standards writers won't like these slashes. We just suggest consumers.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Pardon me?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This was your – Steve, you suggested this be patient/consumers. I suggest we just make it consumers.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes, that's fine. That's fine.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think they're going to like the slash … preference is consumers, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. To be precise, it could be a designated guardian.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's true, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's not always the patient, so I don't know if we want to drift into that language either.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
No. We'll let them worry about that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, we'll let them worry about it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, really.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
…cover it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The only question I want to throw back into the mix is when you say electronic, an electronic format. Do we feel the need to say something about what that format should be, and all I'm concerned is in that it exclude proprietary formats that can't be interpreted, except by limited sources. I want to say a standard format or an accessible format, or a format, as defined in other regs.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Accessible is excellent, excellent because, to John's point, it needs to be accessible to whomever is going to use it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I mean, I think we know it's going to be a CCD/CDA kind of thing, but we ought to probably say something that pushes them in that direction.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If we make it – let me see, electronic accessible format, accessible electronic format.

Sarah Wattenberg – ONCHIT – Public Health Advisor
I think that makes it sound like accessible meaning electronic, not meaning understandable.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sarah, do you have any suggestions?

Sarah Wattenberg – ONCHIT – Public Health Advisor
Why don't you just say…?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm sorry. You could also mean accessible to the consumer, and a CCD is not necessarily very accessible to a consumer.

Sarah Wattenberg – ONCHIT – Public Health Advisor
Maybe you just say in a format that is understandable by the consumer.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, CCD would not be understandable.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. You can't read those things by hand.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes, but provide mechanism by which the CCD is run through a style sheet, and it is accessible, and it is in full fidelity.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, but style sheets is….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
…additional, we would be adding additional expected capabilities, and so….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Keep in mind, if we recommend both of these, number two really takes care of the CCD. That's what that is. It's CCD with a vocabulary that's interoperable. And number one maybe could be focusing exclusively on the consumer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
There are other parts of the reg that actually specifies a format, and maybe we don't have to say anything about it here.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is where … well, this is from the other part of the reg. This isn't from the security section.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So the IFR specifically references CCR and CCD, I believe, as a second choice. I'm sorry, CCD and CCR as a secondary choice. Is that sufficient, or do we reference back to that section?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think, for the consumer, it does.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The reference is for the clinical summary is where the CCD and CCR are mentioned, not for the patient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That clinical summary is – I apologize, I don't have it in front of me – is for whom? Is that specifically provider-to-provider?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, it's Table 2A, the patient summary record.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Yes, those are for provider-to-provider, although the patient can certainly be the conduit, and we want to enable that. I honestly don't think we should bother adding words. I think less is more here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
I think certainly the questions around whether the patient can view it or not will be proven out in the market. I don't think that's something that needs to be legislated. I think we've already said that it needs to be accessible in electronic form.

Sarah Wattenberg – ONCHIT – Public Health Advisor
But isn't the point that it's accessible and understandable?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
I think, operationally, yes. I think if the EHR certification criteria, that's not an easy thing to do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
How do you measure understandable?

Steve Findlay – Consumers Union – Senior Healthcare Policy Analyst
Right. I think….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I think … I think the word "access" itself is intended and expected to be the consumer will be able to access the information, understandable meaning if I get the information in some CCD that I can't see or open, that's not access, that's not electronic access to a copy of my information as a consumer. That might be access to a copy that I can transfer to someone that can do something with it. But I agree. I think less is more here, and using the right words like the word "access" and the word "patient" together allows for confirming and reaffirming the concept that this is access to being provided to the consumer, not to another electronic health record or PHR that has technology to handle CCDs or other formats.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think Sarah is right. Everything we're talking right now is policy, and it really needs to be – there are a lot of policy issues that need to be thrashed out. Let's just focus in on our words here so we're going to make enable a user to provide consumers with electronic access to, what, a view or a copy?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I don't think a view would be appropriate because I think a copy is what we should use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
…that's what the law says. That's a good point. Their clinical information, including blah, blah, blah, then and to obtain a copy of their personal health information in electronic format.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Here's one suggestion to tie in the second part of it because the second part of it is related to access, so I would, instead of saying "and to", I would say, "including the ability to obtain a copy of their personal health information in an electronic format."

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I think that's a good way because I like that. It has to be available, but it's their choice to go get it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You got it. That's what it'll be.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That's a real operational requirement thought, the ability to obtain it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
What do you mean, John?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a good point since this is a certification. Including the ability to—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Provide it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
To provide, not obtain.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. The system must be able to provide a copy.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Good point. Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good point.

Sarah Wattenberg – ONCHIT – Public Health Advisor
This is Sarah. Can I just say one thing?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure.

Sarah Wattenberg – ONCHIT – Public Health Advisor
I know I made the comment about sort of policy stuff, and maybe you don't need to get bogged down on that here, but following on what Walter was saying, I don't know if it's a policy or if it is more implementing what I at least think was the intention, this issue of, it isn't, I don't think, just providing a copy. I do think it's about it being understandable and comprehensible to the consumer. If there's lack of clarity here about what that means, that's going to create, I think, issues in the implementation because, to just provide copies, if they can't understand, I don't think meets the intent.

John Moehrke – Interoperability & Security, GE – Principal Engineer
What is the criteria for understandable? At what level of education? I mean, is it go through some kind of a special filter from a clinical record to consumer friendly terminology?

Sarah Wattenberg – ONCHIT – Public Health Advisor
I know it's – right, that's where it becomes a problematic issue.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The spirit of what we want to say is a standard, nonproprietary format, but we don't really want to get into the business of saying what that means, but we know what it means.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think she's saying, and I'd be happy to this, is human readable. If we say human readable, that doesn't mean that that makes sure that that person can read it, but that a human can read it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I mean, it's really the – hmm.

Sarah Wattenberg – ONCHIT – Public Health Advisor
I'm not sure.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
You know, a raw PDF and a raw XML document are not particularly human readable. It's what programs do to it that makes it readable. And if it's locked down so that you can't – I mean, if it was encrypted such that you couldn't – I mean, we know what we mean in spirit. We want the consumer to be able to use the data. That's why I said usable.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
How about if we said human usable?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I thought we worked our way through that one a minute ago and found something wrong with it, although I don't remember what it was.

John Moehrke – Interoperability & Security, GE – Principal Engineer
What does it mean to use?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
To, you know, make use of, apply utility.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think the best that we can expect of a certification criteria of an EHR is that it has the ability to make the electronic copy available, and to go beyond that really gets into policy, gets into procedure, gets into operational issues, gets into usability issues.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, the word use, when you are creating certification criteria, and then actually executing the certification criteria becomes a huge problem. I mean, how do you demonstrate usability, readability?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. You don't even know what computer they have at home, you know.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
John, I want to throw back some of your complaints, or maybe it was Walter earlier. There is an interoperability issue at stake here. And, in the long-run, we benefit if what the consumers get is as interoperable as what the providers get with respect to the tools like PHRs and other tools. To leave it completely unspecified it to diminish the power of interoperability somewhat. On the other hand, I don't know that we – it's really not our purview to specify what the interoperability standard for consumer data is. I would argue that it's the exact same as what the providers get or what the states get, but that is policy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I've got an idea. Why don't we add a third recommendation that the ONC make it a priority to establish policy around this?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Here's one suggestion because I think we haven't used this in any of the other recommendations. ONC, just like any other federal agencies, have another instrument, which is develop guidance … famous for that, of course, because of HIPAA privacy regulations and security regulations are generic and then OCR publishes guidance that tries to explain in more detail the expectations, the intent.

I think, in leaving it in general terms for this stage, and then recommending that ONC public guidance on the concept of making health information available or enabling consumers to access their health information, what does it mean and what is the intent. I think that would sufficient in this first stage. So using the ability of ONC to produce guidance outside of the regulatory text.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think I'd like to go off of what David kind of said a little bit, I think, which is to say that the electronic format must be at least those, which are specified elsewhere within this regulation, so that we know they will at least get the same format that is specified in the other part.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The patient doesn't want a CCD.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, that would….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well, but wait a minute. You know, absolutely I want a CCD if that's what my PHR can process.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right. But the average patient probably is expecting – if the average consumer who would read that ARRA provision would think they're getting like a Word document or a PDF.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But come on, I mean, if you go to your bank's Web site and download your transactions, they don't come in text files. They come in some Quicken format, and then you load them into an open program that makes them available to you.

John Moehrke – Interoperability & Security, GE – Principal Engineer
In the cases that I'm thinking of, at least in my own personal family's perspective, was that we didn't necessarily need to view the data. We needed to carry the data from one provider to another where they were not otherwise connected, and we had to be the conduit. I don't want to provide the second physician a view of the data. I want to provide them the full fidelity data that they can actually run their decision support engines on.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's one patient.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we spent way too much time on this. If we put in electronic format for the first one, and we add Walter's recommendation for ONC to develop guidance, consumer access to their health information, I think we have it covered.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. The other thing I wanted to say is, I mean, we are dealing with two different things here. One is what the original spirit of it was, which was online access to consumers. It wasn't really the second part, which is obtain a copy so that they can take it to a PHR or to another provider. That's a separate requirement and a separate certification element.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's the requirement, Walter. That's what we've been trying to say. The requirement is an electronic copy, not online access. The requirement is an electronic copy. That's why we've been going around about that. It doesn't say who needs to be able to consume that electronic copy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I wonder if the approach should be similar to what we did when we pushed some of these things to the certification process.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's … certification.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well, but what I'm saying is that when the certification standards, whoever establishes the certification standard could decide, based on, at that time, what is the best practice. Maybe that's CCR this year, and it's CDA level 2 next year, and it's CDA level 3 in five years, and then it's something completely we haven't thought of yet in the future as the best way to create high fidelity transfer of the record.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think we're at that point. I think Walter is right on this one that ONC needs to step up and provide some guidance on consumer access to their health information.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I don't want to carve out consumers as being something special, as in degraded. I mean, I don't think that's right. In other words, whatever the providers get, I want to have too.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then that's what the guidance should say.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And I like that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But I don't think that's really policy. We're not the right group to say that's what it should be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
If policy says, give the consumers a copy of their record, at the consumer's request, and then they say, we'll let the standards committee figure out what that copy should look like.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then we'll take it on.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's already taken care of on Section 170.304F, which is right before G, timely access. F is the electronic copy of health information. Enable the user to create an electronic copy of patient information, including, at a minimum … data in, number one, human readable format. Number two, on an electronic media or through other electronic means in accordance with the standards that are in the IFR 205. So the electronic copy part, I think, is already taken care of.

I think the access part by the consumer, my grandmother trying to see the lab, not downloading it into Quicken, but trying to access and see the lab or see whatever test. That is a different purpose, and that's why I think we're trying to put too much into the timely access that is already taken care of in the previous section on the actual regulation.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
What does that mean, Walter? What are you recommending that we do then?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
What I'm recommending is leaving it, enable a user to provide the patient/consumer with electronic access to a copy of their clinic information, including dah, dah, dah, dah, dah, period. Then recommending for ONC to prepare guidance on expanding the intent around this, but not write it into regulations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But, Walter, I think you're not – where it says ARRA itself, the law itself is what says that they have a right to an electronic copy.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
And the IFR says already the standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, then the standard goes that they'll get online access, and that's the whole crux of what we were discussing … online access….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No, no. Read the letter F, right before letter G, timely access, in the actual regulation, page 2046.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Enable a user, which is an entity, which is an eligible entity, to create an electronic copy of a patient's clinical information, including, at a minimum, blah, blah, blah, in human readable format and on electronic media of – according to the – this has nothing to do with consumers. That's not….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
This is the ability of an EHR to create a copy to give to a consumer .. .someplace else.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, that's what this is. This is the requirement that the EHR be capable to create an electronic copy of a patient … to give to the consumer, to give to another provider, to give to a PHR, to give to the consumer so that they can take the PHR. All that is taken care of with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I see. Yes. They do have the capability to generate … in human readable format.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and I agree that the format that's produced for providers should work for consumers as well in terms of a copy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I don't think the vendors are going to have any trouble building tools to make that useful to consumers through PHRs and, of course, they'll do it through their EHRs. The question then, I think, remains a little bit vague to me is this online access question.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It should be exactly what the law says, electronic copy. But I agree with Walter that that was the cover that they generated in human readable format, so they could give them the same thing. But the online access is not the same as an electronic copy, and the law says electronic copy. The IFR says online access. Those are two different things that we need to bring together.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think we've handled the electronic copy. I think that's fairly clear, so where does the online access trace back to? Is that in ARRA somewhere?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is the first time it appears anyplace. It's not in ARRA.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I thought it was. I'm sorry.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But it is in one of the meaningful use criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think so.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I believe it is.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. You have to give it in 96 hours.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, 96 hours is not online access. You have to give them an electronic copy within 96 hours.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I thought it was that the word online access, I thought I'd seen that, but I don't have it with me.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I certainly hope it isn't restricted to online access.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here. Let's see.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, it wasn't restricted to it. I think it was just one of the ways that you provided it. Of course, the committee yesterday made a whole bunch of recommendations to change some of that too.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, provide attestation online.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
You can go to page 2027, which is Table 1, certification criteria. It says provide patient with timely, electronic access to their health information, including….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, but that's….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Within 96 hours of the information being available to eligible professional.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You're looking in the NPRM?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No. I'm looking in the IFR, page 2027, Table 1, certification criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but what we're trying to say is that's wrong. That has no basis in the law. The law doesn't require online access. The law requires an electronic copy.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It's interesting. It doesn't say online access. This particular table says provide patient with timely electronic access.

Sarah Wattenberg – ONCHIT – Public Health Advisor
That's what meaningful use says.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Then the … when you look at where the word "online" comes to play, they actually the word "electronic access" in the preamble to "online access" in the regulation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's interesting. I see what you're talking about now. Yes. That's yet another reason to change it back to electronic access.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I think that's exactly the point. Enable. The regulation should simply read, enable a user to provide patients with electronic access to their health clinical information, including….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. That just justifies our recommendation more, right? So we revised it so that it's consistent with the earlier words, electronic access to their clinical information. Is that what it says?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Electronic access to their health information, actually is what the meaningful use criteria reads. That's the other concern I had, of course. This particular regulation reads clinical, uses the word clinical information or the term clinical information, and it should probably be with their health information.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, because you might want a copy of your bill as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Okay. We'll change it to provide consumers with electronic access to their health information, including blah, blah, blah. And then we leave….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But don't we want the copy notion in there too because that's also in the law?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm trying to get to … I've overwritten so much stuff here. And to provide a copy of their personal health information in electronic format. Okay. Before anybody jumps in, I'm inking to see my page.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I think that reads very well, and then I would add the second part that I mentioned, provide guidance. ONC should provide guidance on this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Do we want to still include ONC? Yes, I think so too. If we spend this much time on it, it needs guidance. Okay. Standards, encryption and decryption, again, the question about data at rest comes up. So I know that you're going to disagree with this recommendation, so tell me what your thinking is.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We lost you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know what the objection of data at rest is, so in the recommendations, if I delete two, data at rest, and just put encryption and decryption of electronic health information, that's A. Add the capability to encrypt and decrypt information using a symmetric blah, blah, blah … implemented. Then three, two would be exchange the capability to encrypt transmissions must be implemented. Let me see how that differs. I don't think – let's see. John objected to the metric 128 … was on there as number one. Only AES meets that requirement.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Or something proprietary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Or something proprietary. Right. Yes. Now that you're back online, you can….

John Moehrke – Interoperability & Security, GE – Principal Engineer

Obviously the comment that I sent in was that I'd like us to say any encryption algorithm recognized by PHIPS 140-2 annex A, so we're not actually specifying PHIPS criteria. We're saying that it's an algorithm recognized by PHIPS 140-2 annex A, which brings in 3DES and AES, so it meets the encryption criteria that the federal government has to meet anyways, without actually specifying only AES, which is a concern of mine because if we specify only AES, we force everybody to upgrade their operating systems because there are some widely deployed operating systems, especially healthcare, that do not support AES.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
XP does, has a – Microsoft has published an extension. It's probably not an extension. Has published software that allows XP to use AES.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Not for all….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
AES became a standard in 2001, and it is the standard for SMIME, and it's several algorithms. It's a set of algorithms. And I think, you know, 3DES is a remnant of DES, and I think we've been asked to raise the bar, and I think this is an area where we can fairly easily raise the bar because it is widely deployed. AES is very widely deployed. Plus, this is now a final rule, and I don't think, thinking through it, I don't think that we should – I would like to see it actually say AES instead of this symmetric 128-bit blah, blah, blah, but they don't want to do that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Help me out there. They were willing to say SHA-1.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Why are they not willing to say AES? Honestly, if we want to flip over to that argument, I would prefer them to say AES than to say what they've done because what they've done would work perfectly well with a proprietary algorithm that is absolutely unsecure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I totally agree with that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
First off, I would recommend that if they really mean AES, they say AES, as they have with SHA-1.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's a good argument.

John Moehrke – Interoperability & Security, GE – Principal Engineer
But my other concern is still valid. 3DES is recognized by PHIPS 140-2 annex A. I don't understand why this committee thinks that they're smarter than PHIPS.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
PHIPS is carrying that forward, but from the days of yore. But yes, annex A does include 3DES and AES and the third one.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Escrow encryption.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Escrow encryption, yes. To me, I think we either, I'd be perfectly fine going forward and saying we recommend PHIPS 140, use of any encryption standard that is recognized by annex A. That would be fine with me. But I've been told we can't use NIST standards.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Again, we're just pointing at the recommendation of, so I would like to say both of those things. Say, A, we would recommend any algorithm that is recognized by annex A, and B, if they really mean AES, they should say AES.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
John Travis just pointed out to me that the Safe Harbor language in the breach rules does point to PHIPS 140 and does not limit it to AES.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
There is some precedent there. What I'm concerned with is what happens in five years when there's an even better approach. How do we keep the language such that you're not locked into what is today's best algorithm, but won't be necessarily the best after somebody has figured out with quantum computing how to break AES or whatever?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what PHIPS annex A does is, these are the algorithms we recognize so, over time, that would change.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's why I like that reference to somebody that's going to keep it up to date.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Here's what I think. I buy all these arguments. I think that we should mention both the breach rule, and we should mention to the SHA-1 reference, and we should recommend language that says use an algorithm recognized by PHIPS 140-2 annex A. And if you can't do that, then specify AES.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
PHIPS 140 annex A and successor recommendations because they may have an annex B at some point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The purpose of annex A is to keep it up to date, if these are what we recommend.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
All right. That's good. As long as the up-to-date part is implied.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's why they made it an annex instead of part of the reg itself.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I got you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, this is Walter. Going to the actual recommendation language, one concern I have is in the interest of what you described, the capability to do this must be implemented, giving sort of the specific direction to turn on that capability at all time for all purposes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. It's implemented in the product. The other problem that I had with this that I didn't mention and should is that symmetric encryption is not the only way to go. So the way they had it with just AES there and just symmetric encryption, they didn't say that if you use symmetric encryption, you need to use AES. They said use symmetric encryption. Use AES. Essentially that's what they said. And so that would preclude the use of public key encryption to encrypt anything either, and that's why I suggested changing the wording to say the capability to encrypt and decrypt information using a symmetric – so they have to have the capability, but they could also have public key encryption capability as well.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I think that's a low risk problem, but that's not….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, e-mail mostly uses public key encryption. It doesn't use symmetric. I mean, it can, but it doesn't always.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right. I think that's a realistic point.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, but it actually uses a combination, just like TLS.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It uses a combination, exactly right, just like TLC. So the way they had it stated, it did not allow for a symmetric encryption. It just addressed symmetric.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The fact that they broke all of these pieces out becomes troublesome because it's really a proper combination of these things. If you break them out, you can do them horribly wrong and not be secure at all.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Agreed. Do you guys go along with what I just suggested we do?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't mind it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It was your recommendation.

John Moehrke – Interoperability & Security, GE – Principal Engineer

The other piece that I'd like to also clarify is in your exchange item. I'd like to focus the exchange to exchanges intended to cross organizational boundaries.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I don't like it. That is policy.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, but the problem that I have is there's a lot of healthcare network communications today. There is a lot of network communications today that would be very burdensome to….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Absolutely. This sets…. These are standards to be use in products. It says nothing about what you turn on and off in actual use. So it says the product has to be capable of encrypting.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's a certification criteria. That's why all this wording the capability to do this or that is not appropriate in this section on standards. The second on standards should just define the standard itself, not the capability.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. How do you do – so the reason I added the capability to number one is simply so that it didn't sound like all the encryption had to be symmetric. I mean, it could be elliptic curve. There are other encryption … besides symmetric encryption and AES. That can't be just your only one. The way it's written, it is the only one.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I agree there's a problem with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And it said it must be used. Walter, it says here. I'm looking. A symmetric 128 – if we just put AES must be used for symmetric encryption….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Hello?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm still here.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I think we lost Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That would be using their, well, they have a symmetric blah, blah, blah, blah, blah must be used, and I object to that because it won't always be symmetric. But if we said AES must be used for symmetric encryption, it would still be standards language to address your issue, Walter, but it wouldn't lock into AES for everything. So if we changed number one in my recommendation to, "Use an encryption algorithm recognized by PHIPS 140-2 annex A," and if you can't do that, change it to, "AES must be used for symmetric encryption." Then we would delete number two, data at rest. Then we leave – then exchange becomes number three.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
How do you word the exchange? Are we keeping the original language in the regulation, or are we writing the capability to encrypt?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What do they have in the regulation?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It just says an encrypted and integrity protected link must be implemented.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Integrity protection is not encryption. That's a different topic, so we could change this to, "An encrypted transmission link must be implemented." Is that the right language? That doesn't make a transmission link, you know. That precluded end-to-end encryption. That's link encryption, so that's a bad way. I think we leave it like…. But you're right, that is kind of certification language. How would you revise that?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well the last one perhaps, and John might have better wording. An encrypted, well, I would just use the secure communication channel concept for exchange. Secure communication channel must be implemented.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Must be implemented. Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
John, how do you…?

John Moehrke – Interoperability & Security, GE – Principal Engineer
That sounds good.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Is it clear elsewhere that electronic health information is equivalent to individually identifiable health information?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, electronic, they aren't equivalent, oh, so that's their word.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. The concern I would have here is all health information, which means—

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, you're already on the next one?

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, I'm on….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, this is not policy. This is what the product has to be capable of doing, and a product has no sense of context, so a product can't tell whether it's an electronic health information or electronic information or identifiable information. In truth, to be a purist, it should say encryption and decryption of information.

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, not information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Of data, yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
No, we're talking about individually identifiable health information. There is, again, I'll point out, there's a lot of network communications going in and out of the EHR that have nothing to do with any particular patient.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's true, but that's….

John Moehrke – Interoperability & Security, GE – Principal Engineer
An example … vocabulary set.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a policy issue, not a product issue.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, but if we're not specific here, the certification can fail … EHR that doesn't have the ability to encrypt the pulling of a value set.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It doesn't say all electronic health information. It says encryption and decryption of electronic health information. I think that's right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
…the word "all" is put in front of there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Pardon?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Unless it's constrained, the word "all" is put there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, I would argue that a product can't tell what is identifiable and what isn't.

John Moehrke – Interoperability & Security, GE – Principal Engineer
If I'm pulling a value set from a value set registry, I know darn well the value set has no identifiers in it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's not electronic health information.

John Moehrke – Interoperability & Security, GE – Principal Engineer
It certainly is. It's a value set. It tells me what the codes are and what the codes mean. That's health information.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
John, you raise a very good and important point. What's scary about it, of course, is that it cuts across everything in the regulation. Basically when you look at any of the ten certification criteria on security, they all use a term electronic health information. They don't use protected health information, personal health information, identifiable health. They just use the generic term electronic health information across the board on all the certification. This is not just an issue for this particular….

John Moehrke – Interoperability & Security, GE – Principal Engineer
I agree.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's the right term because there are other electronic health information that you do want to be able to encrypt that is not necessarily personally identifiable.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I agree with that. John, in this case, I agree. I think it would be – well, actually, discussed into the NPRM, which calls for as a stage one criteria that protection of electronic health information. So I think, in this case, it probably will cover not just individually identifiable health information, but other health information held by another electronic health record that if accessed then could … some other data become identifiable health information. Even though it might be non-identifiable, it could become identifiable.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, and there are other reasons to encrypt besides just a DHI. I mean, you may want to encrypt. Kaiser may want to encrypt their electronic guidelines. You don't just encrypt PHI and nothing else, so I want to go onto the next one, record actions related to electronic health information. Again, this says electronic health information as well. This is your comment, Walter. The standard calls for auditing of electronic health information is created, modified, deleted, or printed.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, what page are you on? I'm sorry.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's just the next one on page nine.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Nine, okay, thanks.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It says the two concerns are access wasn't included in that list and, second, the auditing of printing would be a challenge for most smaller systems, and even for large systems. It's not likely to include auditing … screens. We recommended adding access to the list of actions, and we recommend deleting printed from the list of actions. And I added this—for 2013, I think they should consider adopting the list of auditable actions and data elements that's in ASTM E-2147. ASTM E-2147 is the same standard that ATNA uses.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO

I'm fine with the recommendations.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I suspect though that the recommendation to just simply remove print will be ignored, and we won't have made progress on the concern you have. I think it's better for us to give them a recommendation that recognizes the discussion you had up above, which is, for those instances where the EHR does know that the information was printed, which I would actually use more generally the word exported.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Exported or outputted, something like that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, so I agree with the concern, especially things dealing with print screens, especially when you're dealing with an EHR that's browser based. You know, the browser can do all kinds of things that you don't have knowledge of, and you have to do all kinds of back flips to stop it from doing that. But where you do know that it has been explicitly exported, you should record….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Let's change it to replace printed with export. I think that's a good argument. It's coming up on the end. We have two minutes to finish this. The cross enterprise authentication recommendations, I think we already talked about this is to replace the SAML XUA with a standard for mutually authenticating the transmission link between entities. The suggested wording is the capability to authenticate the sender and receiver entities for establishing a trusted … between them must be implemented. Walter, that has the same issue you said before. That's really certification….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
The wording in the standard doesn't include the word "capability". The wording in the regulation for this particular standard crosses enterprise authentication. It just says a cross enterprise secure transaction … sufficient information … must be used, so … capability.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, except that I think that's something generally they need to fix. Since the focus of this IFR is on certification criteria for an EHR, it really should be focused on that these are all capabilities and that's….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No, this is not just certification. This is defining the standard for things that might not be or might go beyond certification.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'll just change it to the certification language, Walter, as you suggest. Authenticate the sender and receiver entities before establishing trusted communication paths.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The other thing that we talked about above, and we might as well be parallel, is to indicate that the use of cross enterprise authentication should be road mapped to 2013 or 2015.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'll add that. Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That would be good.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Good point.

John Moehrke – Interoperability & Security, GE – Principal Engineer
If we don't put people on notice, it'll never happen.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and we did it before. We'll do it here as well. The next one is treatment payment and healthcare operations. This is, I again recommend they use ASTM E-2147 as a standard for specifying the data elements and the same thing is John Moehrke's point that the standard needs to … capture the description through post processing rather than real time.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, this one, the only thing, Dixie, that the definition of what needs to be accounted for is already written in the HIPAA regulations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, it is. And the HITECH references the HIPAA regulation or the definition for accounting for disclosure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. I realize that. I think that they should revisit it. The transport standards, both John Moehrke, and myself and I suspect others recommended that those be taken out. First of all, they're both referenced … talk about an area that changes a lot … standard protocols for accessing services. We recommend….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I agree with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I agree. They don't belong there.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Omitted standards, none of us had any objection to their omitting DNS, LDAP, coordinated time, so we said that's fine. But we think that we believe that it may be appropriate to recommend some constraints, some timing constraints for stage two.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, I'm concerned about your recommendation because that's an operational issue. There's nothing that the EHR technology can do about that. That's an operational issue, whether you've set up all of your time synchronization correctly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. I mean, yes, it's something an enterprise decides what they use as a time source. The enterprise decides. But there's a lot in EHR technology covers a broad, broad base. And I think, especially as they go into accounting for disclosures across organizations and as HIEs are implemented, I think they do need to pay attention to time source and time accuracy. I think the other two are taken care of, but I think we should leave that in there. Other people?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We're just basically road mapping it, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I don't have a problem with road mapping it. I'm not sure exactly where it belongs, but somewhere in the … of regulatory environment, it may matter, so just calling it to their attention is probably worth it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. And we recommend that they be considered for stage two.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I mean, it's non-binding. It just puts the issue on the table. They can decide where it fits best.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is accounting for disclosures, as I mentioned. I recommended they look at E-2147 as a list of – and in there, they have a list of what they call basic standards, I think – basic disclosure, elements that need to be captured. And I recommended that they considered using that as the standard. And the … has to do with the post processing and also these, what David calls edge cases where capturing these additional data elements is just silly. I didn't use the word silly, but, you know, where it's obvious what the reason for the disclosure is.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Do we need some clarification that this is a roadmap issue? Is it clear that we're not putting this into the current IFR?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Let me comment because OCR is charged now with defining, and they will be producing that, I assume, on a separate regulation, the actual data elements to be captured.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
By OCR?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO

OCR is going to take care of that part. What I think the expectation was that the technical standard to capture whatever data OCR recommends in their NPRM will be defined here, the technical standard to capture it. Now what data elements, they will be looking at that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So I think ASTM, as a technical standard, would be appropriate. I think that the type of data elements, I would leave it to OCR. Maybe, yes, maybe we can insert here some recommendations for OCR to consider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I'll change the recommend OCR….

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, I think that would be good.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
David, to answer your question, we started off at the beginning. We recommend that they delay its implementation until 2013.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Does it need more roadmap flavor to it?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, I think that's okay, and if it's OCR's call anyway, it's somewhat moot, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Privacy and security gaps, we mentioned again the need to really put something into place for keeping a list of technology standards that are acceptable. This is our general comment. The certification of endpoints, and then the third thing is, both David and I mentioned that the role based access control really should be specified in the 2011 rule. You know, but we think that most vendors – I doubt they add that simply because they can't add anything. You know, they told us that at the last committee meeting, but I guess it can't hurt to mention it. Comments?

Okay, and then the rest is what we're going to put in the different message. All right. I'll let you guys go. Thank you very much for dialing in. Thank you very much for a very useful discussion. I think we've got some really good recommendations to take forward, and you'll see, you know, you'll be copied when I send this to John.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dixie, it's Judy. We need to just make sure there's no comments from the public.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment from the public line?

Operator
Yes. We have a comment from L. Callahan.

Judy Sparrow – Office of the National Coordinator – Executive Director
What is your name and the organization again, please?

M
L. Callahan for HIPIT. I just wanted to draw attention to the reasonableness questions two and three, which you talked about early on. First of all, that breach alerts, real time breach alerts have been available with an … repository since HIMSS 2008 by way of an e-mail to a designated officer such as a compliance officer, and that this is probably a sought after, from a compliance officer standpoint, this is a sought after functionality.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, Dixie. Thanks, everybody.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you, everybody. I look forward to seeing you next week.

Judy Sparrow – Office of the National Coordinator – Executive Director
Bye.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Bye-bye.